



Chicago
New York
Washington, DC
London
San Francisco
Los Angeles
Singapore
vedderprice.com

September 28, 2018

Charles J. Nerko
+1 212 407 6933
cnerko@vedderprice.com

VIA EMAIL

Andrew J. Wronski, Esq.
Foley & Lardner LLP
777 E. Wisconsin Ave.
Milwaukee, WI 53202

Re: *Bessemer System Federal Credit Union v. Fiserv Solutions, LLC*

Dear Andy:

On behalf of Bessemer System Federal Credit Union ("Bessemer"), we write regarding several critical security problems at Fiserv Solutions, LLC ("Fiserv").

Bessemer recently conducted a risk assessment and concluded that it would be necessary to conduct a security review of the privacy and security controls relating to the sensitive non-public member information belonging to Bessemer that is being held by Fiserv. This security review was prompted by a series of highly problematic activities engaged in by Fiserv as well as publicly available reports indicating that Fiserv has recently suffered a security breach affecting the confidentiality of information Fiserv maintains on its customers' behalf.¹

As you are aware, Bessemer is subject to several regulations requiring Bessemer to implement and maintain a reasonable and adequate information security program to safeguard Bessemer's member information. The security review of Fiserv is authorized by federal law, which imposes a duty on a federally regulated credit union such as Bessemer to conduct security reviews of service providers. See 12 C.F.R. Part 748, Appx. A, § III.D.3 ("Each credit union should...[w]here indicated by the credit union's risk assessment, monitor its service providers to confirm they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.").²

We further note that earlier this year, Bessemer requested that Fiserv provide information regarding its information security plans, independent audit reports, and action plan. Fiserv was required to supply all

¹ See Krebs on Security, "Fiserv Flaw Exposed Customer Data at Hundreds of Banks,"

<https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/>.

² See *also*, e.g., NCUA Supervisory Letter 07-01 at 8 ("Credit unions engaging in third party relationships must have an infrastructure (i.e. staffing, equipment, technology, etc.) sufficient to monitor the performance of third party arrangements. In many cases, credit unions outsource processes or functions due to a lack of internal infrastructure or experience. However, outsourcing processes or functions does not eliminate credit union responsibility for the safety and soundness of those processes and functions."); NCUA Letter to Credit Unions 00-CU-11 at 1 ("Institutions should implement an oversight program to monitor each service provider's controls, conditions, and performance.").

Andrew J. Wronski, Esq.
September 28, 2018
Page 2

of this information to Bessemer pursuant to the audit rights granted to Bessemer in the parties' agreement. Fiserv, regrettably, ignored these requests and was unable to provide the required assurances that Bessemer's member information was being properly safeguarded. Consequently, in accordance with Bessemer's federal obligations and duty to protect its members, Bessemer believed it necessary to conduct the security review.

Bessemer's security review revealed several critical security lapses at Fiserv that threaten the confidentiality of Bessemer's member information:

1. Fiserv's system housing member information allows individuals to access member information and register accounts through a trial-and-error process. The security at Fiserv is so lax that Fiserv did not prevent account access through a trial-and-error process (such as by locking out access after multiple several failed attempts, which would be expected). Rather, Fiserv waited for several days before being able to detect this issue—only after numerous days' worth of repetitive, highly anomalous behavior clearly indicative of a security breach. Fiserv thus permits unauthorized individuals to access member information and engage in online banking transactions.

2. Through a trial-and-error process, Fiserv will disclose the last four digits of a member's Social Security Number associated with an account number.

3. In the course of Bessemer's security review, Fiserv apparently added an additional security verification requirement, so that individuals registering for accounts would need to verify a member's house number. This additional security check, however, failed and was readily bypassed because not all of Fiserv's servers were enforcing this requirement.

4. While Fiserv was supposed to enforce a member's acceptance of the terms and conditions before using certain online banking functions, individuals can bypass the screen calling for acceptance of the terms and conditions.

We request that Fiserv immediately identify the four affected accounts so Bessemer can confirm whether they were part of the security review. We further request that Fiserv immediately provide all documents and information concerning the security problems with Fiserv's systems, the accessing of the four affected accounts and transactions conducted on them, documents concerning the presentation and acceptance or non-acceptance of terms and conditions, and the security procedures now in place to safeguard Bessemer's member information and how they have changed over time.

In addition, we note that Fiserv indicated that it is now blocking access to new online banking enrollments. Is Fiserv doing so because there's an ongoing security problem? Please explain the current state of the security of the Fiserv system and why denying access is necessary from a security prospective. Also, is Fiserv suspending new online banking enrollment for other affected Fiserv customers on the shared system? And is Fiserv applying the same security controls to other affected Fiserv customers on the shared system?

We were very disappointed that the security review yielded a multitude of disturbing and serious security problems with a company supposedly as sophisticated as Fiserv. As your last letter urged, "file your complaint and we'll get on with it." Given Fiserv's ongoing and troubling misconduct, which constitutes a pattern of serious security lapses, we look forward to doing so very shortly.

Andrew J. Wronski, Esq.
September 28, 2018
Page 3

Given the severity and time-sensitive nature of this matter, we request Fiserv immediately address this matter and respond to this letter at the earliest possible opportunity, but not later than 9:00 a.m. on October 1, 2018.

This is not an exhaustive statement of all relevant facts and law, and our client continues to reserve all rights in this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read "Charles Nerko". The signature is fluid and cursive, with a prominent initial "C".

Charles J. Nerko